



January 14, 2011

Health Information Exchange Strategic and Operational Plan
Legal and Policy Domain Team
WORKING DRAFT

Contents

1.	Overview	4
2.	Legal and Policy Issues.....	5
2.1	Opt-IN/Opt Out Determination	5
2.2	Data Ownership.....	6
2.3	Data Uses.....	6
2.4	Mandatory Participation	6
2.5	Patient Access to the ND-HIE.....	6
2.6	Oversight.....	7
3	Harmonization of Legal and Policy Issues	8
3.1	North Dakota Century Code § 43-47-09 (Definitions at § 43-47-01).....	8
3.2	The Privacy and Security Rule of the Health Insurance Portability and Accountability Act of 1996 (“HIPPA”).....	8
3.3	Federal 42 CFR Chapter 1 Public Health Service, Department of Health and Human Services, Part 2 Confidentiality of Alcohol and Drug Abuse Records (“42 CFR Part 2”).....	9
3.4	Other Federal Statutes	10
3.5	Bordering State Laws.....	10
3.6	Health Information Strategies	10
4	Education.....	13
4.3	Health Information Strategies and Operational Plans	14
5	Common Forms and Agreements.....	16
5.3	Health Information Strategies and Operational Plans	16
6	Common Policies	18
6.1	Authorization	18
6.2	Authentication.....	18
6.3	Access Control	18
6.4	Audits.....	18
6.5	Breach Notification.....	19
6.6	Patient Right to Request Restriction on Access to and/or Use and Disclosure of PHI..	19
6.7	Accounting of Disclosures.....	19
6.8	Right to Request an Amendment to Health Records.....	19
6.9	Health Information Strategies	20

Health Information Exchange Strategic and Operational Plan
Legal and Policy Domain Team
WORKING DRAFT

1. Overview

The North Dakota Health Information Exchange (ND-HIE) is committed to implementing a secure statewide health information exchange of “protected health information”(“PHI”) that is consistent with state and federal privacy and security laws as well as the Principles articulated in the Office of National Coordinator for Health Information Technology’s, *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information* (“Privacy and Security Framework”).

The Legal and Policy Domain Team of the ND-HIE has considered a number of legal and policy issues that must be addressed in order ensure that a comprehensive privacy and security framework is developed. State and federal laws, including, but not limited to HIPAA and provisions under the Health Information Technology for Economic and Clinical Health Act (“HITECH”) will form the basis for all legal and policy decisions and implementation measures undertaken by the ND-HIE. These issues, strategies and operational plans are summarized below.

In addition, North Dakota is participating in a RTI grant designed to harmonize Legal and Policy issues between North Dakota, South Dakota, Minnesota, Illinois, and Wisconsin. The grant will be used to create standard agreements between the states regarding data use and sharing as well as business associate agreement.

2. Legal and Policy Issues

The Health Information Technology Advisory Committee (HITAC) has formed a Legal and Policy Domain Team to provide assistance during the implementation of the North Dakota HIE Strategic and Operational Plan. The Legal and Policy Domain Team has identified the following policy issues that will need to be addressed in order to implement the North Dakota Health Information Exchange (ND-HIE). Resolution of these issues will require the expertise and input from one or more of the other HIE domain teams, with final decisions made by HITAC.

2.1 Opt-IN/Opt Out Determination

Determining how patient protected health information “PHI” is made available to the ND-HIE is a critical policy decision that needs to be made. “Protected health information” is defined under the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), and is a broad term that essentially includes any individually identifiable health information. There are a number of possibilities to consider:

- The patient’s PHI automatically included in the ND-HIE, with no right to be removed;
- The patient’s PHI is automatically included in the ND-HIE, but patient’s retain a right to have their information not included (the “opt-out” option);
- Patient’s must affirmatively agree to have their protected health information included in the ND-HIE (the “opt-in” option); and
- A combination of any of the above plus the right to place restrictions on specific information.

The Legal and Policy Domain Team recommends default inclusion of patient’s PHI in the ND-HIE with a right to opt-out upon written notification to any participating entity. Default inclusion will initially generate a large number of participants into the ND-HIE. Providing an opt-out option is consistent with the Nationwide Privacy and Security Framework, and the “Individual Choice Principle,” which stresses an individual’s right to make informed decisions regarding their PHI.

The Legal and Policy Domain team recommends limiting a patient’s right to request restrictions on uses and disclosures of their PHI in the ND-HIE to that which is required by law because of the operational and technical challenges related to identifying and tracking requested restrictions. Federal law permits patients to make restrictions on how their PHI is used, but this right is somewhat limited. Under HIPAA, providers are not required to agree to such a request and under HITECH, the restriction is limited to disclosures to health plans where the patient has paid for the service in full (see law more defined under section 6.6 below).

Additionally, the Legal and Policy Domain Team recommends that with the exception of what is required by law for restrictions, an “all or nothing” choice for inclusion into the ND-HIE be adopted. If patients chose to opt out, ALL of their information will be removed or blocked. Like requested restrictions, allowing partial opt-out creates significant operational and technical burdens. The ND-HIE will need to develop a process for addressing requests to restrict PHI as required under HITECH.

The Legal and Policy Domain Team recommends the ND-HIE develop a process that makes it easy for patients to choose to opt back into the ND-HIE if they have initially chosen to opt out. The Legal and Policy Domain Team will create an information booklet that will explain the ND-HIE to consumers, including how their PHI is added in the ND-HIE, the process for opting out of the ND-HIE, and the process for opting back into ND-HIE.

2.2 Data Ownership

Who owns the data is an important policy determination because it establishes responsibilities related to the information (e.g. for purposes of complying with HIPAA) and who would be liable for any potential breaches. The Legal and Policy Domain Team recommends this issue be addressed in any legislation that may be developed.

2.3 Data Uses

The ND-HIE will also need to determine how and for what purposes the PHI in the ND-HIE will be used. The Legal and Policy Domain team recommends the ND-HIE be initially limited to uses and disclosures of PHI for treatment and continuity of care purposes. Limiting the initial uses and disclosures to treatment purposes makes it easier for entities to comply with federal laws and it helps to build trust and gain confidence in the ND-HIE. Once entities participating in the ND-HIE get comfortable with using it for these purposes, HITACH may want to consider expanding the purposes and uses of PHI in the ND-HIE to potentially include public health such public health reporting and surveillance, quality measure reporting, research, and law enforcement.

2.4 Mandatory Participation

Although the state would certainly benefit if all providers were required to participate in the ND-HIE because most patients PHI would then be included in it, the Legal and Policy Domain Team recommends voluntary participation in the HIE, with strong encouragement from the state. A number of stakeholders expressed “big brother” type concerns related to state involvement in the ND-HIE. Trust, collaboration and cooperation are key to successfully implementing the ND-HIE. Given the concerns expressed by many stakeholders, state mandated participation would have the exact opposite effect of fostering trust, collaboration and cooperation.

2.5 Patient Access to the ND-HIE

The Legal and Policy Domain Team will need to resolve the issue of whether patients should have direct access into the ND-HIE. Under HIPAA, patients have a right to access and have copies of their medical records. However, that does not necessarily mean they should have direct access into the ND-HIE like a personal health record.

The Legal and Policy Domain Team recommends patients not be given direct access into the ND-HIE because doing so creates additional security risks and increases the operational burdens of establishing and monitoring passwords. Individual participating providers should

permit patients to see their records and obtain copies if requested. Moreover, the ND-HIE may establish processes that direct patients to where more complete health records may be found. Additionally, individual health care providers or entities participating in the HIE may choose to give patients direct access into their medical records systems.

2.6 Oversight

Consistent with the Accountability Principle of the Privacy and Security Framework, the Legal and Policy Domain Teams recommend HITACH have oversight responsibility of the ND-HIE. This oversight should include ensuring the development, implementation, monitoring, and enforcement of common policies, procedures, forms and Agreements. HITACH must also oversee processes for addressing and mitigating non-compliance and/or breaches in privacy and security standards. Finally, HITACH should ensure that all participants provide employee training on privacy and security policies and procedures and that sanctions be applied for non-compliance with such policies and procedures. The Legal and Policy Domain Team recommends drafting legislation that specifies HITACH oversight responsibilities.

3 Harmonization of Legal and Policy Issues

The Legal and Policy Domain Team recognizes the importance of identifying, analyzing and harmonizing the different state and federal laws affecting access to and release of protected health information within the state and across state lines. North Dakota must follow state (N.D.C.C. § 43-47-09) and federal laws (HIPAA and Federal 42 CFR Chapter 1 Public Health Service, Department of Health and Human Services, Part 2 Confidentiality of Alcohol and Drug Abuse Records (“42 CFR Part 2)) when determining what protected health information may be released and under what circumstances (e.g. whether patient authorization is required). However, it will be important for the North Dakota HIE to also have an understanding of any bordering state laws that are either contrary to or more stringent than the laws North Dakota must follow. The following laws will need to be reviewed, harmonized and analyzed:

3.1 North Dakota Century Code § 43-47-09 (Definitions at § 43-47-01)

This statute establishes confidentiality provisions for “counseling” services rendered by a “counselor” as both terms are defined under this chapter. Specifically, this statute states: “except as authorized by law, no person licensed under this chapter may be required to disclose any information acquired in rendering counseling services without the consent of the person who received the counseling services.”

“Counseling” is defined as: “the application of human development and mental health principles in a therapeutic process and professional relationship to assist individuals, couples families and groups in achieving more effective emotional, mental, marital, family and social or educational development and adjustment. The goals of professional counseling are to:

- Facilitate human development and adjustment throughout the lifespan;
- Prevent, assess and treat emotional, mental or behavioral disorder and distress which interferes with mental health;
- Conduct assessments for the purpose of establishing treatment goals and objectives; and
- Plan, implement, and evaluate treatment plans using professional counseling strategies and interventions.

“Counselor” is defined as “a person who had been granted either a professional counselor or associate professional counselor by the board.” “Board” means “the board of counselor examiners”

3.2 The Privacy and Security Rule of the Health Insurance Portability and Accountability Act of 1996 (“HIPPA”).

The HIPAA Privacy Rules establish minimal requirements for the use and disclosure of PHI. Under these rules, PHI may be accessed, used and/or disclosed without patient authorization for treatment, payment or health care operations purposes. The HIPAA Security Rules establish minimum security requirements for creating, maintaining and exchanging electronic protected

health information. Provisions under HITECH strengthened the HIPAA Security Rules and expanded coverage of the requirements to additional entities. These rules will provide the basis under which the ND- HIE operates.

3.3 Federal 42 CFR Chapter 1 Public Health Service, Department of Health and Human Services, Part 2 Confidentiality of Alcohol and Drug Abuse Records (“42 CFR Part 2).

42 C.F.R. Part 2 broadly protects *all information* about any person who has applied for or has been given a diagnosis or received treatment for alcohol or drug abuse at a federally assisted program (“Program”). Program means “an individual or entity, or an identified unit within a general medical facility that holds itself out as providing, and provides alcohol or drug abuse diagnosis, treatment or referral for treatment.” Program also means “medical personnel or other staff in a general medical care facility that are identified as having a primary function of providing alcohol or drug abuse diagnosis, treatment or referral for such treatment.” Federally assisted means “conducted, regulated or directly or indirectly assisted (e.g. pays for services) by any department or agency of the United States.”

Information created and maintained at a Program may not be disclosed unless the patient has provided written consent or unless another very limited exception specified in the Statute applies.

The only treatment related exception to the consent requirement is “to medical personnel to the extent necessary to meet a bona fide medical emergency.” Under this exception, information may be disclosed to medical personnel who have a need for the information for the purpose of treating a condition “which poses an immediate threat to the health” of the individual and “which requires immediate medical intervention.”

It is important to have a good understanding of this statute because if this statute applies, in general, any information subject to it can only be accessed and/or disclosed pursuant to patient written authorization. Moreover, this statute places additional restrictions on the information subject to it, such as a prohibition on redisclosure (unless specifically permitted) and a requirement that certain statements be appended to any information disclosed.

Recently, the Substance Abuse and Mental Health Services Administration of the U.S. Department of Health and Human Services (the agency that wrote 42 CFR Part 2) published a guidance document entitled, “Frequently Asked Questions, Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange.” This guidance document will have to be reviewed and analyzed, with recommendations coming from the Legal and Policy Domain Subgroup.

3.4 Other Federal Statutes

The Legal and Policy Domain Team must also review and analyze additional federal statutes to determine any impact they may have on activities and processes contemplated by the North Dakota HIE. These may include (depending on the purposes for which the HIE will ultimately be used), but are not limited to:

- The Federal Privacy Act (5 U.S.C. § 552a);
- The Freedom of Information Act (5 U.S.S. § 552; also 45 C.F.R. Part 5)
- Medicaid Privacy Requirements (42 U.S.C. §1396a(a)(7) and 42 C.F.R. §§ 431.300-307)
- Genetic Information Nondiscrimination Act of 2008 (GINA) (Pub. L. No. 110-233)
- Clinical Laboratory Improvement Amendments (42 U.S.C. §263a and 42 C.F.R. § 493.1291)
- Controlled Substances Act (21 U.S.C. § 801 and 21 C.F.R. § 131623)
- Federal Policy for the Protection of Human Subjects (45 C.F.R. §§ 46.11(a)(7), 46.116(a)(5))
- Federal Certificate of Confidentiality (research subjects) (42 U.S.C. 241(d))
- Family Educational Rights and Privacy Act (1974) (20 U.S.C. § 1232h, also 34 C.F.R. Part 99)
- AHRQ Confidentiality Provisions (42 U.S.C. §§299c-3(c),(d))
- CDC Confidentiality Provisions (42 U.S.C. § 242m(d))
- Patient Safety and Quality Improvement Act of 2005 (42 U.S.C. 299b-21 to 299b-26, also, 42 C.F.R. Part 3)
- The Patriot Act (109 P.L. 177)

3.5 Bordering State Laws

The North Dakota HIE will need to review and analyze the privacy and release of information laws from bordering states such as Minnesota (which is known to have stricter laws), South Dakota, and Montana to determine whether contrary or more stringent provisions exist that may impact the exchange of protected health information with these bordering states.

3.6 Health Information Strategies

The Legal and Policy Domain Team recommends the following strategies and creates the following operational plans for resolving these issues:

- North Dakota Century Code § 43-47-09
 - HITAC will request a state level attorney (e.g. Attorney General or other appropriate designee) formally review and draft an opinion that addresses the following in relationship to the ND-HIE:
 - 1) Whether patient consent *is required* in order to release PHI protected by this statute for the purposes contemplated by the ND-HIE.

- 2) If consent is required, must it be in writing and if so, what is required for a valid consent.
- Harmonizing State and Federal Laws
 - The Legal and Policy Domain Team will create a legal work group to analyze and make recommendations regarding regulatory requirements in relationship to ND-HIE activities. HITACH will determine who and what stakeholders should be represented on the work group.
 - The legal workgroup will utilize any existing documents already addressing these issues including, but not limited to:
 - 1) Analysis, spreadsheets and/or PowerPoint presentations prepared by state attorneys.
 - 2) *Frequently Asked Questions, Applying the Substance Abuse Confidentiality regulations to health Information Exchange*, prepared by the Legal Action Center for the Substance Abuse and Mental Health Services Administration of the U.S. Department of Health and Human Services Administration;
 - 3) The Office of National Coordinator for Health Information Technology's, *Federal Privacy Laws Table*;
 - 4) The Office of National Coordinator for Health Information Technology's, *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information* ;
 - 5) Any other guidance documents developed by Office of National Coordinator for Health Information Technology; and
 - 6) Any other analyses or reports of these issues from other identified intra and interstate resources
 - Given time constraints and other limitations, the legal workgroup may consider outsourcing analysis and coordination of these activities to a consulting or legal firm with recognized expertise with these laws and regulations.
 - The legal workgroup will identify any legal barriers to the electronic health information exchange and will consider suggesting legislative changes to better align with efforts and goals of the ND-HIE.
 - Bordering State Laws
 - HITACH and/or the Legal and Policy Domain Team will reach out and establish on-going relationships with corresponding workgroups and state leaders in bordering states. Developing and maintaining these relationships is important North Dakota because it will allow the state to:
 - 1) Efficiently learn about bordering state laws;
 - 2) Identify potential barriers to interstate electronic exchange; and
 - 3) Collaboratively develop processes for the electronic exchange PHI in common bordering areas.

Health Information Exchange Strategic and Operational Plan
Legal and Policy Domain Team
WORKING DRAFT

- Actively participate in the Upper Midwest HIE State Health Policy Consortium Project.

4 Education

Both consumers and providers will need to be given education related to the North Dakota Health Information Exchange (ND-HIE). The type, detail, format and modalities will differ between the two groups.

4.1 Provider Education

Health care providers will need education addressing the following:

- Meaningful use;
- The ND-HIE generally; and
- Rules and regulations governing access to and disclosure of PHI

Achieving meaningful use by a large number of entities is critical to the development and success of the ND-HIE. To that end, the Legal and Policy Domain team recommends HITAC take a leadership role in collaborating with current exiting entities to help achieve this goal. Meaningful use education is currently provided by the Center for Rural Health with the University of North Dakota. HITAC should work with the Center for Rural Health to ensure meaningful use education is broadly available to all types of providers in the state, not just primary care providers.

It was clear during the environmental scan that not all health care providers had the same level of understanding about HIE generally, the ND-HIE specifically, or its impact on them. Additionally, it was clear that entities had differing opinions about how and when state law, HIPAA and other federal laws applied to release of information. HITAC will need to consider creating education modules that incorporates state law, HIPAA and other relevant federal laws and explain how PHI may be used and disclosed within the ND-HIE. Modalities for delivering some education needs to be explored, but may include internet modules, webinars, audio conferences, and public services announcements.

4.2 Consumer Education

Public forums were held in four cities in North Dakota during the environmental scan. Questions and comments presented during the environmental scan demonstrated an overall lack of knowledge by consumers of health information exchange in general and an overarching concern for maintaining the privacy and security of individual health records. Additionally, many consumers expressed concern over who would have access to their information, especially whether the state and/or federal government would have access. Based on these forums, consumer education should focus on the following:

- The purpose and benefits of ND-HIE;
- How their medical information will become part of the ND-HIE and how it will be protected;
- Who has access to their information; and

- Whether the federal and/or state government will have access into their health information stored and shared within the ND-HIE.

Consumer education should be developed at 8th grade level to ensure most of the population can understand it and should be delivered using multiple modalities, which may include written materials, public forums and media presentations.

4.3 Health Information Strategies and Operational Plans

The Legal and Policy Domain Team recommends the following strategies and creates the following implementation plans for consumer and provider education:

- Provider Education
 - The Legal and Policy Domain team will collaborate with the Center for Rural Health to ensure providers understand meaningful use and how to achieve meaningful use status. This includes:
 - 1) Determining any education gaps based on what the Center for Rural Health is currently doing;
 - 2) Determining methods and identifying potential resources available to provide additional education; and
 - 3) Developing a plan to address additional educational needs.
 - Engage provider associations (e.g. hospital, medical, nursing, pharmacy etc.) to help educate their respective constituents by:
 - 1) Identifying and recommending the associations that will be approached to help deliver this message;
 - 2) Recommending a plan for making contact and follow through; and
 - 3) Drafting an educational document that can be used by the associations (helps ensure a consistent message is delivered).
 - Create content and coordinate the delivery of more public methods for educating providers.
 - 1) Develop content that can be used to consistently deliver the education; and
 - 2) Consider Public Service Announcements or other public radio or television announcements that help deliver the message.
 - Develop and deliver content that specifies what can and cannot be done in ND-HIE under North Dakota, HIPAA and other federal release of information and privacy protection laws.
 - 1) Content should be easy-to understand and limited to practical every day information in summary format in order to keep the providers engaged and to ensure they understand the most critical legal issues pertaining to their involvement in the ND-HIE;

Health Information Exchange Strategic and Operational Plan
Legal and Policy Domain Team
WORKING DRAFT

- 2) Consider delivering content in multiple formats;
 - 3) Collaborate with professional associations (e.g. medical, nursing, hospital, pharmacy etc.) to ensure content gets added to relevant conferences; and
 - 4) Consider making content available to meet continuing education requirements.
- Consumer Education
 - The Legal and Policy Domain Team will develop the following consumer based educational content pieces:
 - 1) Consumer booklet or pamphlet. The booklet or pamphlet will be used by all entities participating in the ND-HIE. It will be written in an 8th grade level or lower and will also be made available other languages common to a particular area in the state.
 - 2) A summary document to be used by health care providers and consumer advocacy groups. This document will be easy-to-understand and in summary format to ensure that consumers are receiving consistent information about the ND-HIE.
 - 3) Content for use in a public campaign. Public information content will explain the ND-HIE in simple, easy-to-understand terms.
 - The Legal and Policy Domain Team will engage the health care provider community, including applicable associations, as well as consumer advocacy groups (e.g. AARP, Triple A etc.) to help educate consumers about the ND-HIE by:
 - 1) Identifying and recommending the associations and advocacy groups that will be approached to help deliver this message;
 - 2) Recommending a plan for contact and follow-through; and
 - 3) Utilizing the summary document to ensure a consistent message is delivered.
 - Create content and coordinate the delivery of more public methods for educating providers.
 - 1) Develop content that can be used to consistently deliver the education; and.
 - 2) Consider Public Service Announcements or other public radio or television announcements that help deliver the message.
 - Make content available in multiple formats to help meet continuing education requirements (medical, nursing, pharmacy etc.).
 - 1) Identify and plan a process for getting continuing education credits.
 - 2) Identify methods and implement a process for delivering content (e.g. webinars, internet modules etc.).

5 Common Forms and Agreements

The North Dakota Health Information Exchange (ND-HIE) must develop a set of forms and Agreements that all HIE participants may use. Developing a common set of forms and Agreements will create consistency and help foster trust, coordination and cooperation among all entities participating in the HIE.

The following is a list of potential (not all inclusive) list of forms and Agreements that may need to be developed depending on policy decisions made by HITAC. The Legal and Policy Domain Team will take the lead in making recommendations related to such forms and Agreements.

5.1 Forms

- Consent Form to Opt into the ND-HIE
- Form to Opt out of the ND-HIE
- Form Allowing Restrictions on the Access to and Use or Disclosure of Protected Health Information
- Patient Consent for the Release Protected Health Information (as applicable)
- Breach Notification Letter
- Model Notice of Privacy Practices
- Request for Amendment to PHI
- Accounting of Disclosures
- Patient Requests for Audit
- Request for Access to HIE

5.2 Agreements

- End User Agreements
- Business Associate Agreements
- Participant Agreement
- DURSA

5.3 Health Information Strategies and Operational Plans

The Legal and Policy Domain Team recommends the following strategies and creates the following implementation plan for addressing this issue:

- Research and Collect Forms created by existing HIE's
 - The Legal and Policy Domain Team will research the Internet and contact bordering states for additional sample forms and Agreements as necessary.
 - Forms and Agreements may be made available as part of participating in the Upper Midwest HIE State Health Policy Consortium
- Determine the extent to which sample forms can be modified for use by the ND-HIE

Health Information Exchange Strategic and Operational Plan
Legal and Policy Domain Team
WORKING DRAFT

- The Legal and Policy Domain Team will provide initial review and recommendations for modifications or additions to all collected forms and agreements.
- Contract with external legal or consulting firm to create final drafts of all forms and agreements.
- Firm must have current expertise in reviewing and drafting these forms and agreements.
- Provide recommendations for final approval of all forms and Agreements by HITAC.

6 Common Policies

The ND-HIE must develop and enforce policies that comply with the Privacy and Security Rules under HIPAA and HITECH and are consistent with the Principles articulated under the Privacy and Security Framework. HIPAA establishes minimum requirements governing the privacy and security of protected health information for all deemed “covered entities.” Additionally, provisions under HITECH strengthen these requirements and expand the types of entities that must adhere to some of the requirements (e.g. “business associates”). While these federal laws create baseline privacy and security requirements, not all of the entities that may participate in the HIE are required to follow these regulations. Moreover, entities inconsistently interpret and apply these requirements. Developing (and enforcing) a core set of policies and procedures is imperative to establishing trust among participants in the HIE.

The Legal and Policy Domain Team recommends the ND-HIE develop and implement policies addressing the following:

6.1 Authorization

Authorization refers to the process by which an entity determines who has the right to access protected health information. Entities typically apply a “role-based” process to establish an individual’s right to access protected health information. Role based access takes an individual’s role or job into consideration and their need to access information in order to perform their job. An authorization process is consistent with the Safeguards Principle under the Privacy and Security Framework.

6.2 Authentication

Authentication refers to the mechanism by which an individual granted access to the ND-HIE can be verified as that individual. The most common method for authenticating individuals is through the use of unique passwords. Developing a process for authenticating individuals is consistent with the Safeguards Principle under the Privacy and Security Framework.

6.3 Access Control

Access control policies ensure that individuals granted access to the ND-HIE only access the information needed to do their job or what they may be allowed by patient authorization. Developing an access control process is consistent with the Safeguards Principle under the Privacy and Security Framework.

6.4 Audits

Audits are performed to identify areas of inconsistent or inadequate levels of compliance with state and federal laws as well as common policies, procedures and contractual obligations. Consistent audit practices enhance confidence and trust in the privacy and security of the ND-HIE. Developing an audit process is consistent with the Safeguards Principle under the Privacy and Security Framework.

6.5 Breach Notification

The HITECH rules require entities to develop processes for notifying individuals when their electronic PHI is “breached” (situation must meet the definition of a breach). As such, the ND-HIE must adopt a breach notification process. Providing notification of a breach is consistent with the Openness and Transparency Principle of the Privacy and Security Framework.

6.6 Patient Right to Request Restriction on Access to and/or Use and Disclosure of PHI

The HIPAA Privacy Rule grants patients the right to request that a covered entity restrict how their PHI is used or disclosed for treatment, payment or health care operations purposes. However, under these rules, a covered entity is not required to agree to a restriction.

Effective February 18, 2010, provisions under HITECH allow a patient the right to request, and requires the health care provider to comply with a request to restrict disclosures of PHI to a health plan for purposes of payment or healthcare operations when the PHI pertains to a service for which the healthcare provider has been paid in full by the patient “out of pocket.” Granting patients a right to request restrictions as required by HITECH is consistent with the Collection, Use and Disclosure Limitation Principle in the Privacy and Security Framework.

6.7 Accounting of Disclosures

Currently, the HIPAA Privacy Rule grants patients a right to request an “accounting” (or a listing) of disclosure of their PHI. However, disclosures made for “treatment,” “payment” or health care operations do not have to be included as part of this accounting. In general, disclosures made for treatment, payment and healthcare operations purposes account for at least 90% of all disclosures of PHI, and would comprise, most, if not all disclosures contemplated by the ND-HIE.

Effective January 1, 2014, entities must be able to account for disclosures of *electronic* PHI for treatment, payment and health care operations purposes. This change in law will have a direct impact on the ND-HIE. Consequently, the ND-HIE must have a process for meeting this requirement. Having an accounting of disclosures process is consistent with the Openness and Transparency Principle of the Privacy and Security Framework.

6.8 Right to Request an Amendment to Health Records

The HIPAA Privacy Rule grants patients the right to request an amendment to their PHI contained in a “designated record set” (as defined by HIPAA). This is consistent with the Correction Principle under the Privacy and Security Framework. The HIPAA Privacy Rule establishes requirements for developing processes that implement this patient right. The ND-HIE will need to develop a policy that meets these requirements.

6.9 Health Information Strategies

The Legal and Policy Domain Team recommends the following strategies and implementation plan for creating and implementing common policies:

- Research and collect sample policies created by existing HIE's or other related entities
 - The Legal and Policy Domain Team will research the Internet and contact bordering states for additional sample policies and procedures as necessary.
 - The Legal and Policy Domain Team will review the Office of National Coordinator for Health Information Technology's, *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information* and any other related guidance documents to ensure all policies and procedures are consistent with principles articulated in the documents.
 - Sample policies and procedures may be made available as part of participating in the Upper Midwest HIE State Health Policy Consortium
- Determine the extent to which sample policies and procedures can be modified for use by the ND-HIE
 - The Legal and Policy Domain Team will provide initial review and recommendations for modifications or additions to all collected forms and Agreements.
- Contract with external legal or consulting firm to create final drafts of all forms and Agreements.
 - Firm must have current expertise in reviewing and drafting these forms and Agreements.
- Provide recommendations for final approval of all policies and procedures by HITAC.